BECAUSE YOU ASKED ENTRIES June 2010

Q: What do I need to know about Telephone Security?
A: The first rule - classified information must never be discussed over unsecured (unencrypted) telephones. Attempts to "talk around" classified information by using personally devised code words, references, paraphrasing, etc. is strictly prohibited. When using telephones approved for classified discussions, either a STU or STE, remember to do the following:
- ensure the person on the other end has the appropriate access authorization (clearance) and the need-to-know,
- make sure that the classified portion of your conversation is not overheard by uncleared personnel in your office or the immediate area,
- remember, most offices are not soundproof, and voices tend to carry into adjacent offices/areas and hallways, for this reason you must always check these areas prior to discussing classified, to make sure it is safe to do so, and finally,
- devices approved for classified discussions, STU-III & STEs, must be located in either a Limited or Exclusion Security Area at the Headquarters.

Q: What is the difference between a security infraction and a security violation?
A: A *security infraction* is any knowing, willful, or negligent action contrary to the requirements of Executive Order 12958, Classified National Security Information (soon to be superseded by the President's new Executive Order 13292), as amended does not constitute a "violation."

Examples of security infractions are:
- Leaving classified documents or material exposed and unattended or unsecured, to include leaving a classified container open and unattended.
- Failing to properly safeguard classified documents or combinations to security containers.
- Changing a document's classification marking without proper authority.
- Destruction of classified document in other than the prescribed manner.
- Improper transmission of classified documents or material.
- Failure to report known or suspected incidents of security concern.
- Failure to escort uncleared persons within a Security Area.

Although this is not an all inclusive listing of security infractions it is some of the more common ones. Committing a security infraction may result in administrative discipline, including loss of access authorization. If it is found that an individual's gross negligence resulted in one of these incidents or similar infractions the action may constitute a security violation resulting in criminal prosecution or other administrative actions taken against the guilty party.

Any action or intent that constitutes a violation of U.S. law or Executive Order or the implementing directives is a *security violation*. Suspected or known violations of U.S. criminal statutes, federal statues, or federal laws pertaining to the unauthorized disclosure of classified matter are referred to federal law enforcement for further action.

Contact your HSO or consult the Headquarters Facility Master Security Plan for additional information on security infractions and violations.

Q: What are the requirements for access to classified information?
A: Access to classified information is granted only to those who possess the appropriate access authorization and who require access in the performance of official or contractual duties - the operative word here is "official." Just as the holder of the information is responsible for its protection, he/she is also responsible for releasing/disseminating classified matter appropriately. If you pass classified matter to another individual you must ensure two things: 1) the recipient has the right security clearance, and 2) he/she has a need-to-know, i.e. requires this information to do their job - for official business.

Q: What exactly is the "need-to-know" and what does it mean?
A: Need-to-know is a determination made by an authorized holder of classified or unclassified controlled information that a prospective recipient requires access to the specific classified or unclassified controlled information in order to perform or assist in a lawful and authorized Government function. All employees have the duty to adhere to the "need-to-know" policy as part of their personal security responsibilities. Check with your supervisor if there is any doubt in your mind as to an individual's "need-to-know."

NOTE: No person may have access to classified information unless he or she has been granted an access authorization equal to or higher than, the classification level and category of the information, and the requisite "need-to-know." Additionally, no person is entitled to access classified information solely by virtue of their rank, office, position, or security clearance.

Q: What exactly is a security area?
A: Classified matter must be processed, discussed, handled, or stored in security areas that provide adequate protection measures. Buildings and rooms containing classified matter must have the security measures necessary to detect and deter unauthorized persons from gaining access to the information. This includes security measures to deter persons outside the facility protective zone from viewing or hearing classified information. Confining classified activities to approved security areas is an integral part of the Headquarters protection strategy.

Two security areas that you should be familiar with are Limited and Exclusion:

Limited Area – Limited Areas are security areas designated for the protection of classified matter. Limited Areas are defined by physical barriers encompassing the designated space and access controls to ensure only authorized personnel are allowed to enter and exit the area. A means must be provided to detect and deter unauthorized entry into the Limited Area.

Exclusion Area – An Exclusion Area is a security area established for protection of classified matter, where mere presence in the area would normally result in access to classified information. The boundaries of Exclusion Areas must be encompassed by physical barriers that detect and deter unauthorized entry. Exclusion Areas require access controls that ensure only authorized personnel are allowed to enter and exit the area.

Q: What is a vault-type (VTR) room?
A: A DOE HQ approved room having combination-locked doors and protection provided by an approved intrusion alarm system activated by any penetration of walls, floors, ceilings, or openings, or by motion within the room. In a sense, a VTR is like a walk-in security container. Individuals must be authorized for access to all classified matter within the VTR before they are allowed to enter.

Q: How do I establish a security area?
A: Once you determine that you require a security area for conducting classified activities, your HSO must initiate the following steps to obtain approval:

• A Security Area Request/Facility Information Worksheet (available in Section 6, HQMFSP) must be completed and forwarded to the Office of Security Operations, HS-1.31.

• Members from the HQ Survey Team will conduct the appropriate physical security review and produce a report identifying required protection measures as necessary.

• Upon determination that the area meets all protection requirements, a security area approval memorandum and certificate will be transmitted to the requesting HQ Element.

NOTE: Once a security area has been approved, two things can affect its continued approval. First, any physical changes to the area may affect the integrity of the security posture in place at the time of approval. Second, security areas are approved for specific classified activities at specific classification levels and categories. If there are any changes to the classified activities or classification levels of the approved activities, the HSO must submit a new security area approval request.

Q: What security forms do I need in a security area?
A: There are four forms you should be familiar with and have posted in the security area:

- SF 700, Security Container Information, Part 1 & Part 2: used to identify personnel responsible for the container (who to contact in case of emergency) and to record security container combinations (respectively). Remember, Part 2 which is used to store the combination must be handled and marked to the highest level of the classified matter stored in the container. Part 1 is usually stored in the locking drawer of the container. *You must ensure this information is current and you know where Part 2 is stored.*

- SF 701, Activity Security Checklist: provides a systematic means of recording end-of-day room/area security checks. The SF 701 is usually stored within the security area.

- SF 702, Security Container Check Sheet: this forms records the times, dates and initials of individuals who have opened, closed, or checked a particular container, room, or vault. The SF 702 must be affixed to security container or entrances to security areas and vault type rooms. At HQ facilities, the form is not required for card reader-controlled Limited Security areas with video surveillance and/or alarmed doors.

- Optional Form (OF) 89, Maintenance Record for Security Containers and Doors: this form is used to keep a record of all maintenance and servicing performed on the container. It is stored inside the locking drawer. In spite of its name, it is not optional.

Q: What should I do if I spot something suspicious or out of place?
A. On May 1, 2010, a New York City Times Square street vendor observed a suspicious vehicle parked in a no-standing zone with its hazard lights on and the engine running. He reported the suspicious activity (SAR) to police who responded to the scene. Police observed smoke billowing from vents of the vehicle, popping noises, and the smell of gunpowder. The vehicle was found to contain a vehicle-borne improvised incendiary device (VBIID).

Alert citizens and business officials could avert a potential terrorist or criminal incident by observing and reporting a suspicious vehicle. In 2007, an ambulance crew saw smoke coming from a green Mercedes, near the Tiger Tiger nightclub in London and reported the vehicle to police. Investigators discovered a considerable amount of explosive material and material intended to be shrapnel in the vehicle. Often times vehicle bombs or vehicle borne improvised explosive devices (VBIED) display outwardly visible indicators.

Anyone who observes these indicators should immediately call the police:

1. Vehicles that appear to have an unusually heavy load in the trunk should be considered suspicious.
2. Smoke, fumes, or strong odors emanating from the vehicle.
3. Propane tanks, gas cans, wires, timing devices, or other unusual cargo in the passenger compartment of a vehicle. Additionally, unauthorized vehicles parked in restricted areas should immediately be investigated and removed.

Emergency Telephone Numbers

In the Forrestal, Germantown, Cloverleaf, and 955 L'Enfant buildings, dial extension 166 for emergencies. In the 270 Corporate and 950 L'Enfant buildings, dial 9-911.

Non-Emergency Numbers

Germantown, Cloverleaf, and the 270 Corporate Center dial: 3-2403; Forrestal dial: 6-6900; 950 L’Enfant Plaza dial: 202-863-7901; and 955 L’Enfant Plaza dial: 202-485-3350.